AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to Fig. 7. This sheet replaces the original sheet. In Fig. 7, "CONNET" has been replaced with --CONNECT--.

Attachment: Replacement sheet
Annotated sheet showing changes

REMARKS

Claims 1-50 are pending in the present application. Claims 1, 7, and 45-48 have been amended. Claims 1, 5, 7, 8, 10, 11, 15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, 32, and 45-48 are independent claims. The Examiner is respectfully requested to reconsider the various rejections in view of the above amendments and following remarks.

Interview on June 20, 2006

Applicants thank Examiner Ellen Tran for taking the time to discuss the present application with Applicants' representative, Jason Rhodes (47,305), during the personal interview on June 20, 2006. The substance of the interview is provided below.

Claims Discussed: Claims 1, 7, and 45-48 were discussed.

Prior Art Discussed: U.S. Patent No. 5,796,836 to Markham (hereafter "Markham") and U.S. Patent No. 6,226,742 to Jakubowski et al. (hereafter "Jakubowski")

Proposed Amendments: Applicants proposed the amendment of claim 1 implemented above. Applicants proposed amending claim 7 in a similar manner (as implemented above).

General Results: Agreement was reached that the proposed amendments of claims 1 and 7 would overcome the § 102 rejection of those claims in view of Markham. No agreement was reached as to the § 102 rejection of claims 45-48, although the Examiner agreed to reconsider these rejections in view of the arguments presented by Applicants.

Specification

In the Amendment filed December 30, 2005 (hereafter "Previous Amendment"), Applicants attempted to amend the last paragraph of page 28. This amendment was intended to change "IT" to --IV--. However, due to typographical error, the amendment mistakenly indicated that "IV" was being changed to --IT--. Thus, the specification has been amended above to correct

this typographical error. Applicants submit that no new matter is being introduced by this amendment.

Drawings

In the Previous Amendment, Applicants intended to correct Fig. 7 by replacing "CONNET" with --CONNECT--. However, as noted by the Examiner in the outstanding Office Action, the replacement sheet was inadvertently omitted from the Previous Amendment. Thus, attached hereto is a replacement sheet and annotated copy of Fig. 7 incorporating the above correction.

Rejection Under 35 U.S.C. § 102

Markham Rejection

Claims 1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, and 41-44 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Markham. This rejection is respectfully traversed.

Independent Claims 1 and 7:

Independent claim 1 has been amended as proposed during the interview of June 20, 2006. Similar amendments have been made to independent claim 7. Since the Examiner agreed that these amendments overcome the rejection, Applicants respectfully submit that independent claims 1 and 7 are in condition for allowance, and claims 2-4, 33, 41, and 43 are allowable at least by virtue of their dependency on claims 1 and 7.

Independent Claims 5, 11, 15, 17, 21, 23, 27, and 29:

As to independent claims 5, 21, and 23, Applicants respectfully submit that these claims recite elements for effectively interrupting the encryption process of one set of logically continuous data elements in an encrypting unit/module/step with an encryption process of other data.

Instead, Markham discloses a system that **decouples** the encryption of one plain text block from the encryption of the next plaint text block (col. 3, lines 36-38). In other words, Markham teaches using different encryption processes (corresponding to different pseudorandom vectors) to encrypt successive plain text blocks. Since Markham is concerned with taking advantage of multi-processor techniques, Markham **teaches away** from encryption processes that sequentially encrypt logically continuous data elements (see col. 5, lines 36-50). Thus, Markham does not teach or suggest interrupting the encryption process between logically continuous data elements with an encryption process of other data.

In the Response to Arguments (Office Action at page 2), the Examiner asserts, "[Markham's] decoupling just as in the claimed invention removes the dependence on the first data element to be encrypted before the second element starts the encryption process." However, this is a mischaracterization of Applicants' invention. The present invention is not intended to remove any dependency between data elements in an encryption process. Thus, when logically continuous data elements are being encrypted according to the present invention, the encryption of a particular element may still be dependent on the preceding element. However, the invention does allow such an encryption process to be interrupted by another encryption process.

At least for the reasons given above, Applicants respectfully submit that Markham fails to anticipate the features of claims 5, 21, and 23.

As to independent claims 11, 15, 17, 27, and 29, Applicants point out that these claims recite elements for interrupting the decryption process of logically continuous data elements in a decrypting unit/module/step with a decryption process of other data. Thus, for reasons similar to those set forth above, Applicants respectfully submit that Markham fails to anticipate the features of claims 11, 15, 17, 27, and 29.

Jakubowski Rejection

Claims 45-50 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Jakubowski. This rejection is respectfully traversed.

Independent claims 45 and 47 recite an encryption apparatus/method in which each block of ciphertext data output from the encrypting unit/step is input to the message authentication code (MAC) generator/generating step. These claims further recite that the MAC generator/generating step starts generating the MAC before the blocks of plaintext data have been encrypted by the encrypting unit/step.

Similarly, independent claims 46 and 48 recite a decryption apparatus/method in which each block of plaintext data output from the decrypting unit/step is input to the MAC generator/generating step, and that the MAC generator/generating step starts generating the MAC before the blocks of ciphertext data have been decrypted by the decrypting unit/step.

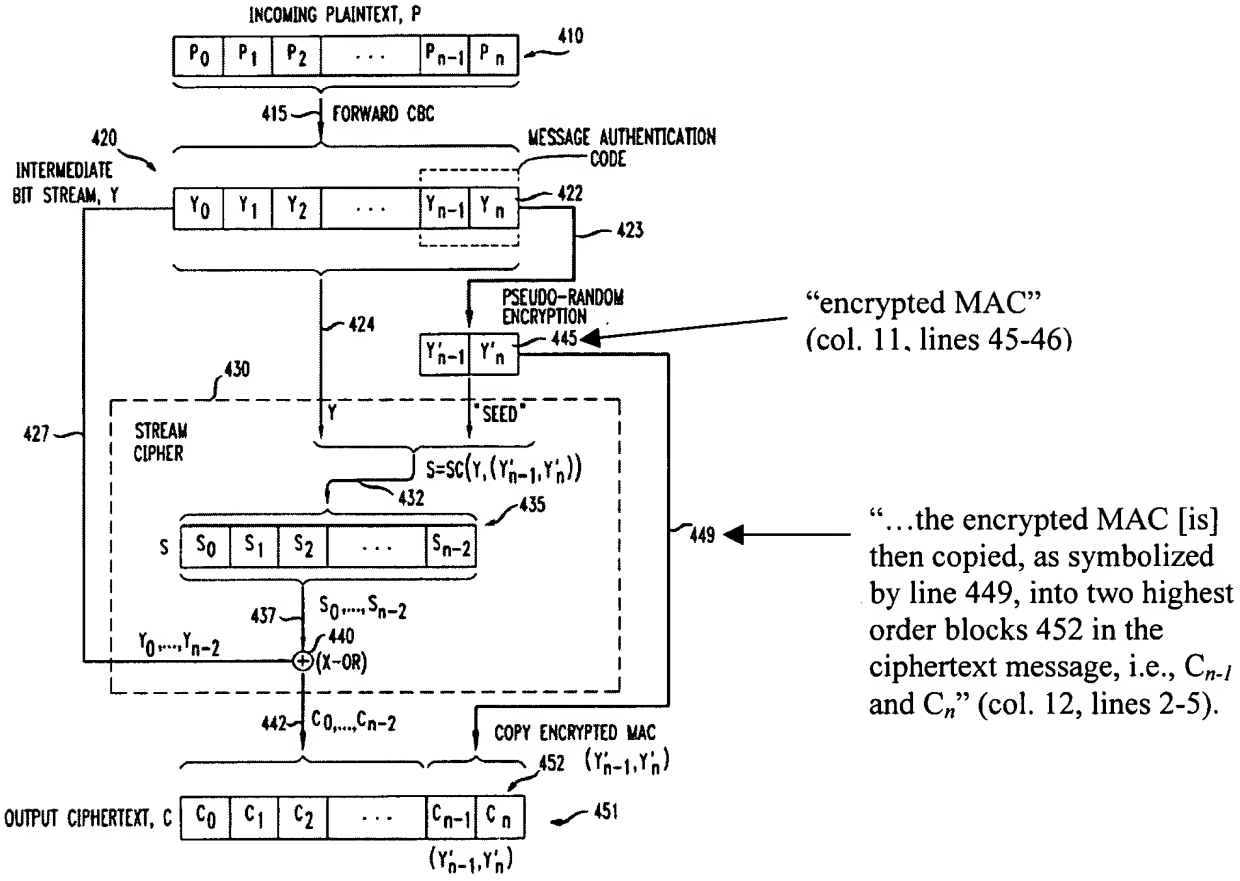
Applicants respectfully submit that Jakubowski fails to disclose the aforementioned features.

Independent Claims 45 and 47:

As to the encrypting apparatus/method of claims 45 and 47, Jakubowski's encryption process generates the MAC using an intermediate bit stream, which is generated **before** a single ciphertext block is generated.

This is particularly shown in Fig. 4A of Jakubowski, which is reproduced below along with some annotations to link certain parts of the figure to corresponding portions of Jakubowski's text.

Fig. 4A of Jakubowski (Annotated)



As shown in this figure, Jakubowski's invention first generates an intermediate stream Y_0 ... Y_n from the plaintext data. Then, Jakubowski's invention concatenates the last two blocks Y_{n-1} and Y_n of the intermediate stream, and encrypts the concatenated blocks to form the MAC (Y'_{n-1}, Y'_n). See col. 9, lines 34-50. This encrypted MAC is

In fact, in Jakubowski's encryption process, it is *impossible* for the output ciphertext blocks to be inputs for generating the MAC, since Jakubowski uses the MAC to generate each ciphertext block. As shown in Fig. 4A, Jakubowski's invention uses the MAC as a "seed" to

encrypt the intermediate bit stream and, thus, generate the ciphertext $C_0 \ldots C_{n-2}$. See, col. 10, lines 30-34.

At least for the reasons given above, it is respectfully submitted that Jakubowski does not teach each and every feature in independent claims 45 and 47.

Independent Claims 46 and 48:

As to claims 46 and 48 (decrypting apparatus/method), Jakubowski states, "[d]ecryption proceeds in a reverse fashion" (col. 9, lines 58-59). Thus, Applicants respectfully submit that claims 46 and 48 are not anticipated by Jakubowski.

§ 102 Rejections Should be Withdrawn

At least for the reasons set forth above, Applicants submit that independent claims 1, 5, 7, 11, 15, 17, 21, 23, 27, 29, and 45-48 are allowable at least for the reasons given above. Accordingly, Applicants submit that claims 2-4, 6, 12-14, 16, 22, 28, 33, 35, 37, 39, 41-44, 49, and 50 are allowable at least by virtue of their dependency on allowable independent claims. Thus, reconsideration and withdrawal of each rejection under § 102 is respectfully requested.

Rejection Under 35 U.S.C. § 103

Claims 8-10, 18-20, 24-26, 30-32, 34, 36, 38, and 40 stand rejected under 35 USC § 103(a) as being unpatentable over Markham in view of Jakubowski. This rejection is respectfully traversed.

Markham/Jakubowski Fails to Teach Every Claimed Limitation

Initially, Applicants point out that MPEP § 2143.03 sets forth the following requirements for a proper rejection under 35 U.S.C. § 103:

> To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Applicant respectfully submits that the prior art fails to provide a teaching or suggestion of all of the features in the claimed invention.

Independent Claims 8, 10, 24, and 26:

As to independent claims 8, 10, 24, and 26, these claims recite ciphertext block data C_i, which is identical to the ciphertext block data C_i output from the encrypting unit/step, is input to the MAC generator/generating step.

The Examiner relies on Jakubowski for these features (see, e.g., Office Action at pages 3-4). However, for reasons discussed above in connection with claims 45-50, Jakubowski does **not** input a ciphertext block to the MAC generator/generating step. As shown above with respect to Jakubowski's Fig. 4A, Jakubowski's MAC is actually used as an input (or "seed") for generating the ciphertext blocks. Thus, Applicants respectfully submit that the Examiner has failed to provide a teaching in the cited references of every limitation in claims 8, 10, 24, and 26.

Independent Claims 18, 20, 30, and 32:

Independent claims 18, 20, 30, and 32 recite a MAC generator/generating step, which feeds back an intermediate MAC result and receives ciphertext block data as input. These claims further recite that C_i is input to the MAC generator/generating step before the ciphertext block data C_{i+1} is decrypted by the decrypting unit/step.

Again, the Examiner relies on Jakubowski for these features. Applicants respectfully point out that Jakubowski's decryption process in Fig. 4B, rather than Fig. 4A. Jakubowski describes the process of Fig. 4B in detail in col. 12, line 39 – col. 13, line 39.

As described in these sections, Jakubowski's invention decryption process first generates a decrypted MAC 473 by extracting and decrypting (using inverse DES) the last two blocks C_{n-1} and Cn of the incoming ciphertext message (see col. 12, lines 39-46). However, since this step does not feedback an intermediate MAC result, it cannot be relied on to teach the claimed MAC generator/generating step.

Jakubowski further teaches that, after the entire plaintext message 490 is recovered, the plaintext message is subjected to forward CBC in order to recover the MAC 483. Accordingly, the process for generating this MAC 483 does not begin until after all of the ciphertext blocks C_0 ... C_n have been decrypted. See col. 13, lines 20-27. Thus, Jakubowski's process for generating MAC 483 cannot be relied on to teach the claimed MAC generator/generating step because it does not input one ciphertext block data C_i before the ciphertext block data C_{i+1} is decrypted.

Thus, Applicants respectfully submit that the Examiner has failed to establish a *prima facie* case with respect to independent claims 18, 20, 30, and 32.

§ 103 Rejection Should be Withdrawn

At least for the reasons set forth above, Applicants submit that independent claims 8, 10, 18, 20, 24, 26, 30, and 32 are allowable. Accordingly, claims 9, 19, 25, 28, 31, 34, 36, 38, and 40 are allowable at least by virtue of their dependency on allowable claims. Thus, reconsideration and withdrawal of this rejection is respectfully requested.

Conclusion

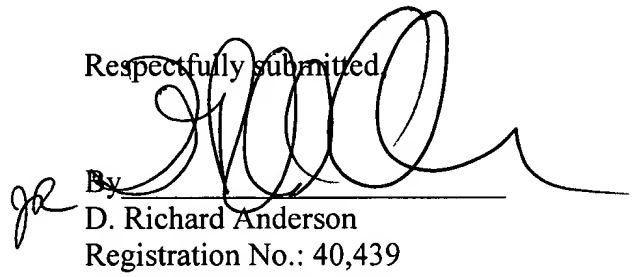
Entry of this Amendment After Final is respectfully requested. In view of the above amendments and remarks, the Examiner is respectfully requested to reconsider the outstanding rejections and issue a Notice of Allowance in the present application.

However, should the Examiner believe that any outstanding matters remain in the present application, the Examiner is respectfully requested to contact Jason W. Rhodes (Reg. No. 47,305) at the telephone number of the undersigned to discuss the present application in an effort to expedite prosecution.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Dated: July 6, 2006

Respectfully submitted,



By
D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant

Attachments

Fig. 7